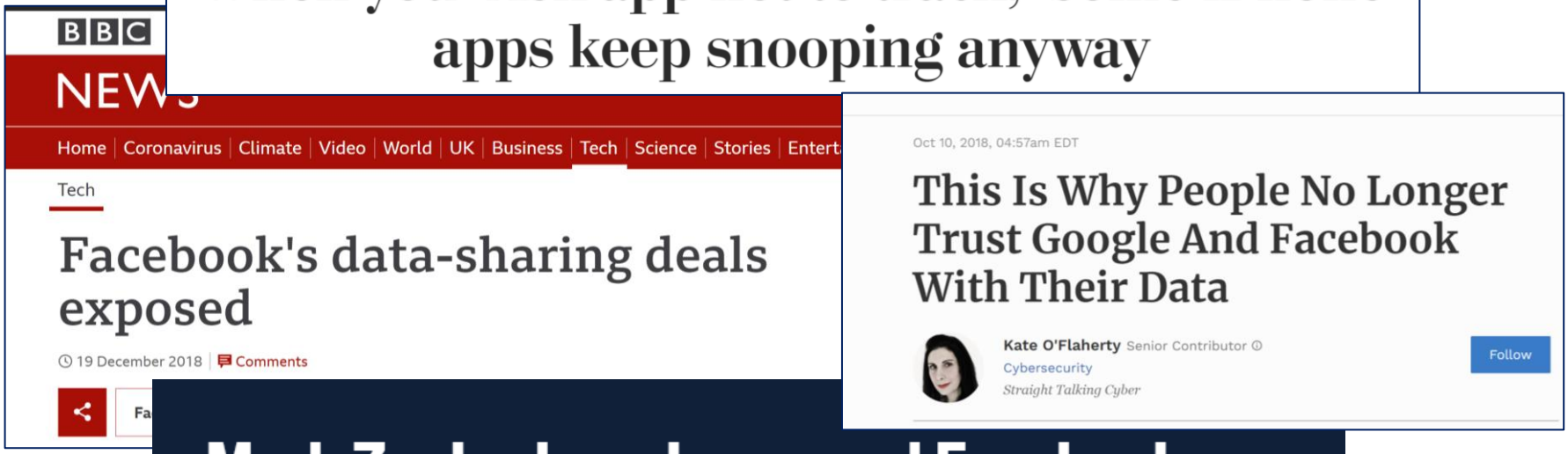
Data Protection Laws

Languages and computer systems department

University of Seville

Introduction



Why data matters

ics/cambridge-analytica-scandal-fallout.html

The New York Times

Cambridge Analytica and Facebook: The Scandal and the Fallout So Far

Revelations that digital consultants to the Trump campaign misused the data of millions of Facebook users set off a furor on both sides of the Atlantic. This is how The Times covered it.

The Times reported that in 2014 contractors and employees of Cambridge Analytica, eager to sell psychological profiles of American voters to political campaigns, acquired the private Facebook data of tens of millions of users — the largest known leak in Facebook history.

MARCH 24

Another look at 'Brexit'

The Times and The Observer reported allegations that the 2016 "Brexit" campaign used a Cambridge Analytica contractor to help skirt election spending limits. The story implicated two senior advisers to Prime Minister Theresa May. Testifying to Parliament a few days later, a former Cambridge employee, Christopher Wylie, contended that the company helped swing the results in favor of Britain's withdrawal from the European Union.

annoyance at how tech giants use personal information. As one of the affected Facebook users put it, "You are the product on the internet."

When data is put to good use

Big data is helping to solve this problem, at least at a few hospitals in Paris. A white paper by Intel details how four hospitals that are part of the Assistance Publique-Hôpitaux de Paris have been using data from a variety of sources to come up with daily and hourly predictions of how many patients are expected to be at each hospital.

Once again, an application of big data analytics in healthcare might be the answer everyone is looking for: data scientists at Blue Cross Blue Shield have started working with analytics experts at Fuzzy Logix to tackle the problem. Using years of insurance and pharmacy data, Fuzzy Logix analysts have been able to identify 742 risk factors that predict with a high degree of accuracy whether someone is at risk for abusing opioids.

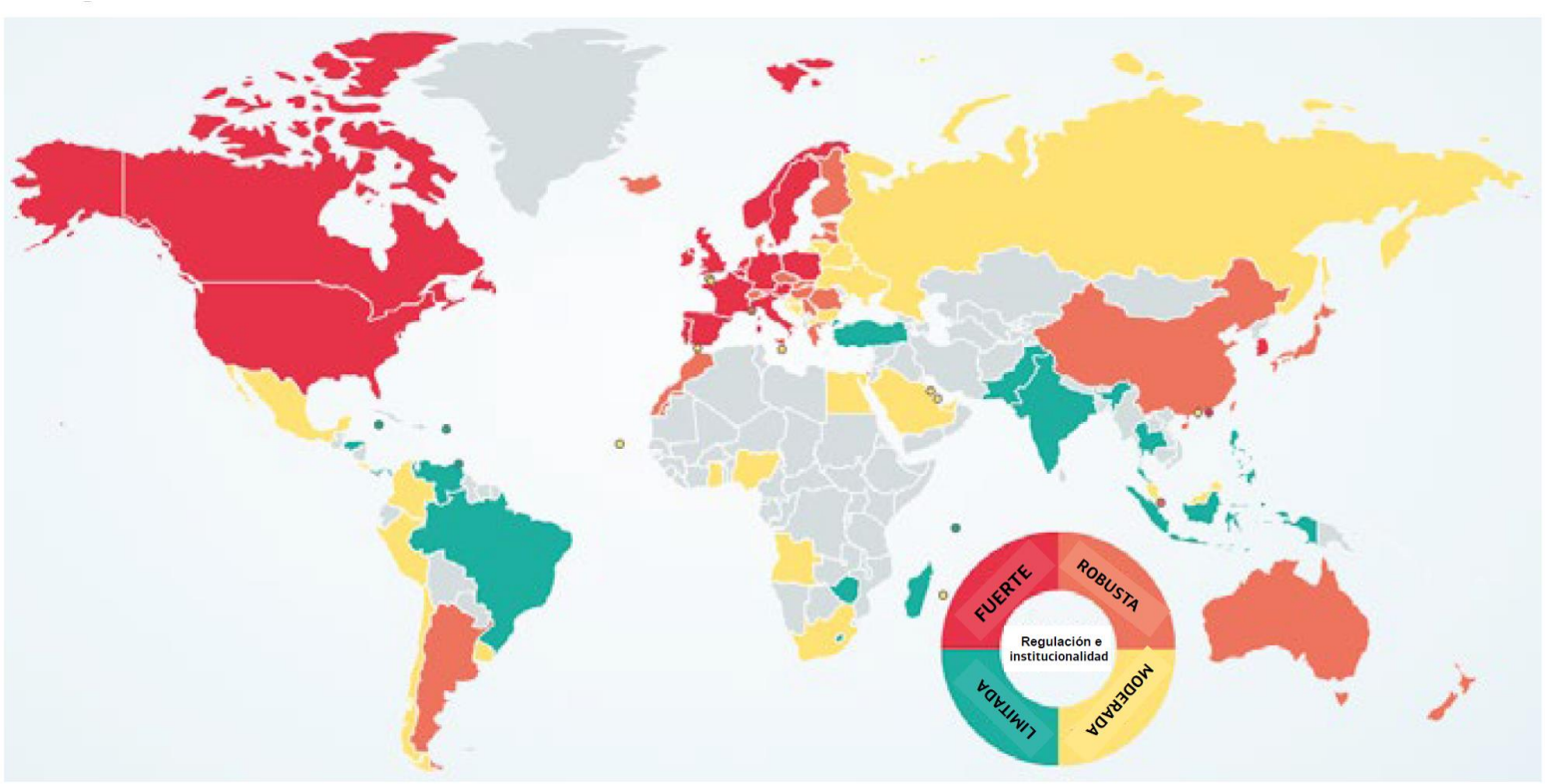
Medical researchers can use large amounts of data on treatment plans and recovery rates of cancer patients in order to find trends and treatments that have the highest rates of success in the real world. For example, researchers can examine tumor samples in biobanks that are linked up with patient treatment records. Using this data, researchers can see things like how certain mutations and cancer proteins interact with different treatments and find trends that will lead to better patient outcomes.

This data can also lead to unexpected benefits, such as finding that Desipramine, which is an antidepressant, has the ability to help cure certain types of lung cancer.

Conclusions: Regulation

- The collection and automated processing of people's data should not be prohibited, but regulated so that this use is made within sensible limits and with full respect for the rights of users.
  - Legitimate purposes
  - Clear information
  - Safe storage
- It is essential to monitorize data transfers to other organizations, both inside and outside the E. U.
- Existing regulation for applications in the Spanish territory includes:
  - European rules
  - Spanish rules

Data protection in the world



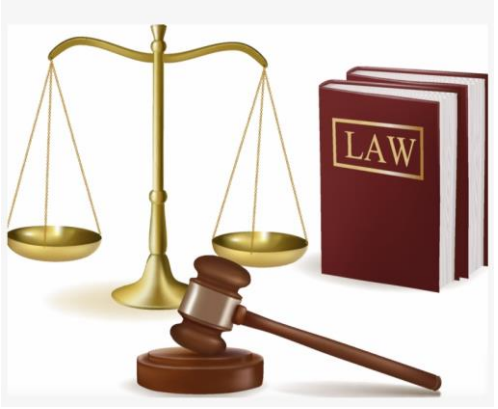
Fuente: 2017 DLA Piper.

Roadmap

1. **Rule hierarchy**
2. European rules
    1. GDPR
3. Spanish rules
    1. Constitution
    2. LOPDGDD

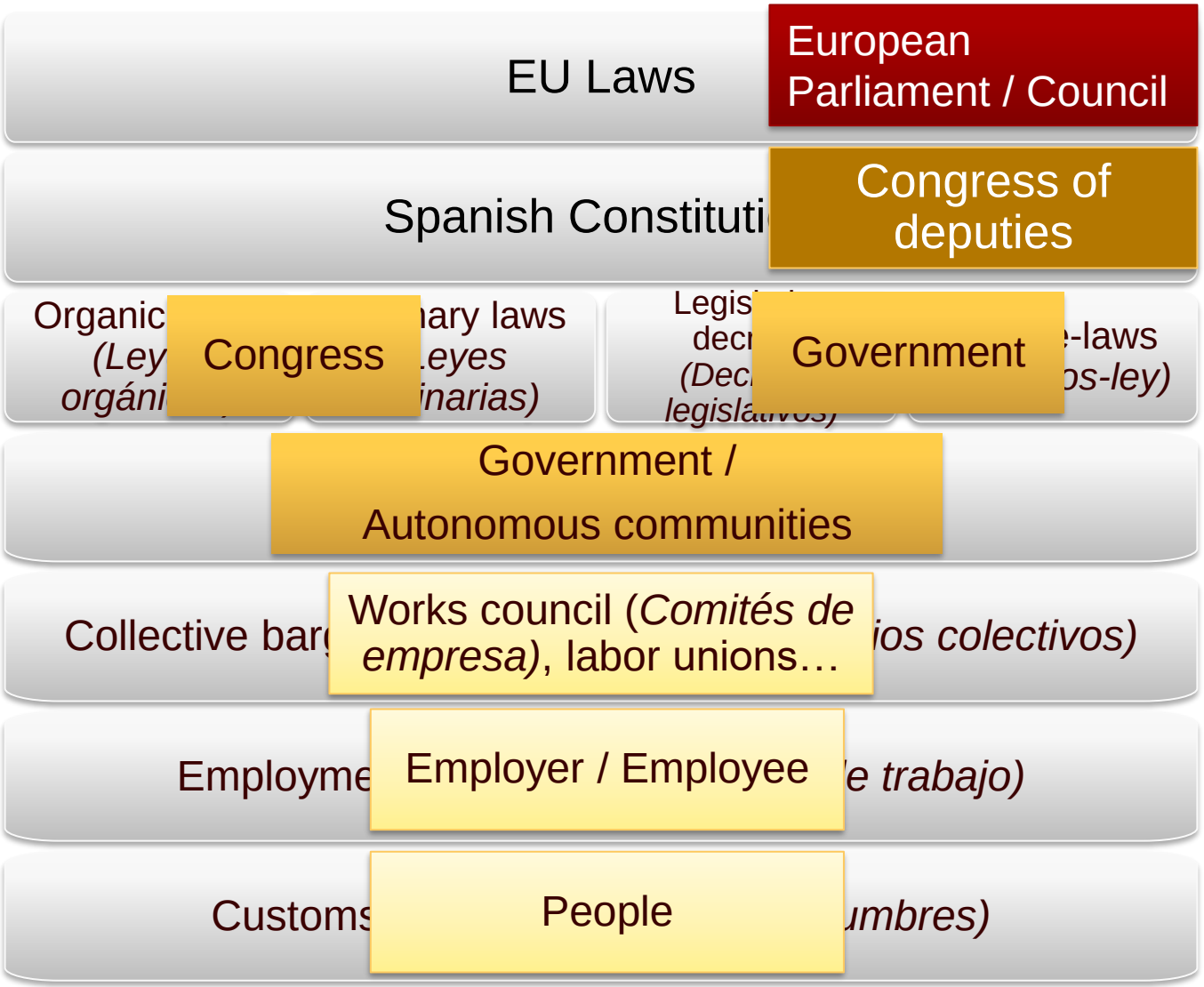
Hierarchy of laws

- The law is legislation created and enforced through social or governmental institutions to **regulate behavior**.
- Law is made up of a set of rules of **unequal weight**. The force of law of these rules follows the principle that a **hierarchy** of norms exists. Therefore, in applying a law, one must make sure that a given rule does not contradict a principle of law that is superior to it
- **European Union** law is a system of rules operating within the member states of the European Union



Spanish legal system

Spanish legal system - authorities



Roadmap

1. Rule hierarchy
2. European rules
    1. **GDPR**
3. Spanish rules
    1. Constitution
    2. LOPDGDD

The scope


Countries
EU - Yes/Schengen - Yes
EU - No/Schengen - Yes
EU - Yes/Schengen - No
ICELAND
NORWAY
SWEDEN
FINLAND
RUSSIA
ESTONIA
LATVIA
LITHUANIA
DENMARK
IRELAND
UNITED KINGDOM
NETHERLANDS
BELARUS
POLAND
GERMANY
UKRAINE
BELGIUM
CZECH REP.
SLOVAKIA
LUXEMBURG
MOLDOVA
FRANCE
SWITZ
LIECHT.
AUSTRIA
HUNGARY
ROMANIA
SLOVENIA
CROATIA
ITALY
BOSNIA & HERZ.
SERBIA
SAN MARINO
BULGARIA
ANDORRA
MONACO
MONTENEGRO
KOSOVO
NORTH MACEDONIA
ALBANIA
PORTUGAL
SPAIN
VATICAN CITY
TURKEY
GREECE
CYPRUS
LEBANON
ISRAEL
MOROCCO
ALGERIA
TUNISIA
MALTA

General Data Protection Regulation (RGPD)

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the **protection of natural persons with regard to the processing of personal data and on the free movement of such data**, and repealing Directive 95/46/EC
- Became effective May 25th, 2018

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

Personal data

Any information relating to an identified or identifiable natural person ('data subject');

*an identifiable natural person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

(Art. 4 RGPD)

Processing

*Any operation or set of operations which is performed on personal data or on sets of personal data, **whether or not by automated means**, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*

(Art. 4 RGPD)

Profiling

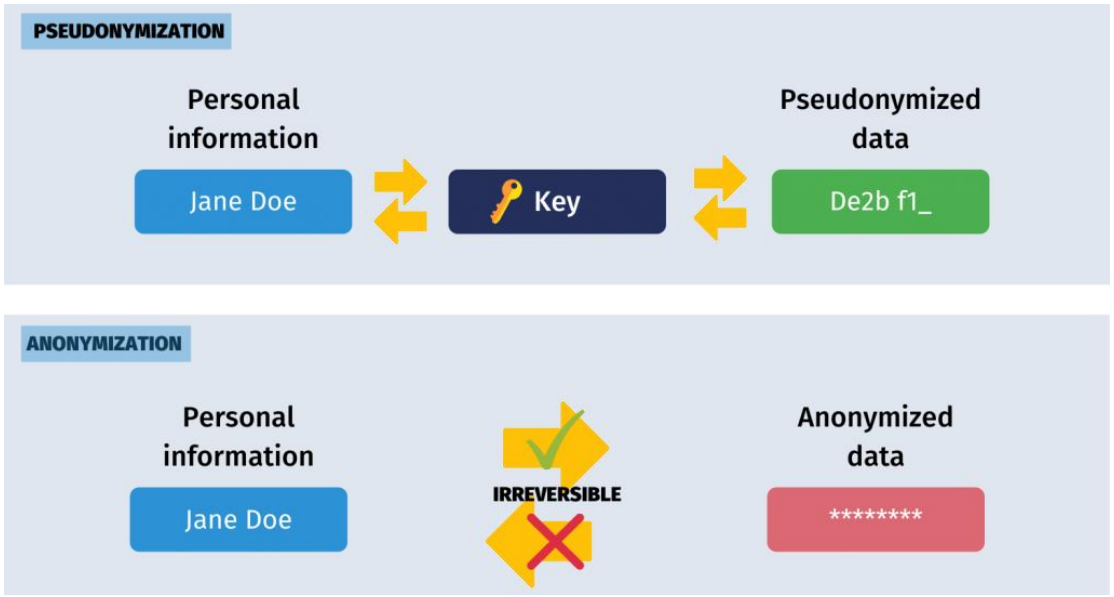
*any form of automated processing of personal data consisting of the use of personal data to evaluate certain **personal aspects** relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;*

(Art. 4 RGPD)

Pseudonymisation

*The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is **kept separately** and is subject to technical and organisational measures to ensure that the personal data are **not attributed** to an identified or identifiable natural person;*

(Art. 4 RGPD)



Supervisory authority

the natural or legal person, public authority, agency or other body which, alone or jointly with others, ***determines the purposes and means of the processing of personal data****; where the purposes and means of such processing are determined by Union or Member State law;*

(Art. 4 RGPD)

- Spanish Data Protection Agency *(Agencia Española de Protección de Datos, AEPD)*
  - Operating since 1994
  - Oversees the compliance with the legal provisions on the protection of personal data. The agency is headquartered in the city of Madrid and it extends its authority to the whole country.
  - https://www.aepd.es/en/

Scope

- The GDPR applies to:
  - All the previously defined personal data, which refer to an identifiable person
    - It is possible to pseudonymize/anonymize data for specific types of processing
      - Statistics, scientific or historical research…
- It is specially appliable to:
  1. Special categories of data, such as those that reveal the ethnic or racial origin
  2. Child data
- It does **not** apply to:
  1. Anonymous information, i.e., information that does not refer to any identified or identifiable natural person,.
  2. Anonymized data.
  3. Personal data of deceased people (each member State should regulate them)
  4. Data about a company (**legal person**)
  5. Service providers outside the E.U.

Obligations

- Lawful, transparent and fair processing of data
  - Using data with a **legitimate purpose**, only for that purpose, and informing the users about the purpose
- Limited use of data
  - Storing only necessary data, only for the necessary period of time
- Establishment of sufficient data protection measures
  - Data encryption, secure communications…
  - Protection againt accidental losses
- Recording of security violations
  - Companies have to notify every security violation to the supervisory authority (AEPD)
- Privacy by design
  - data protection in data processing procedures is best adhered to when it is already integrated in the technology when created.
- Safe data transfers to third parties
- Data protection officer
- ARCO-POL rights
- Obtaining explicit consent from the users

Data protection officer

- Mandatory when:
  - Processing is carried out by a **public authority** or body, except for courts acting in their judicial capacity;
  - Processing of **large-scale** data (how large?)
  - Specific types of processing needed for **certain businesses** (LOPDGDD, Art 34)
- Tasks
  - Inform and advise the controller or the processor and the employees who carry out processing of their obligation
  - Monitor compliance with the GDPR
  - Provide advice when requested as regards the data protection impact assessment
  - Cooperate with the supervisory authority (AEPD)
  - Act as the contact point for the supervisory authority on issues relating to processing
- Designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks
- May be a staff member.
- The processor shall publish the contact details of the data protection officer (AEPD)
- Participate in all issues related to data protection
- Does not receive instructions regarding the exercise of the tasks
- Cannot be dismissed or penalized for performing the tasks
- Bound by secrecy or confidentiality
- May fulfil other tasks and duties, if there is no conflict of interest

ARCO-POL rights

Access	•request and obtain information free of charge regarding whether his/her personal data is being processed, for what purpose and specific uses, the origin of the data, whether it has been transferred or is intended to be transferred and to whom
Rectification	•amend, free of charge, their personal data when it is inaccurate or incomplete
Cancellation	•cancel or erase, free of charge, their personal data when it is inadequate, excessive or unnecessary, or when it is stored for a period in excess. Implies blocking & deletion
Objection	•request, free of charge, that the processing of their personal data not be carried out
Portability	•receive your data in a structured electronic format and usual use to be able to transmit them to another responsible
Oblivion	•(Right to be forgotten) obtain from the controller the erasure of personal data concerning him or her without undue delay
Limitation of treatment	•not to be the subject of automated individual decisions

Consent for transfers

- In general, **explicit consent** is needed for dat transferring.
- There are certain situations in which explicit consent is **not** needed for data transfer, e.g.:
  - When the processing is needed for executing a contract in which the user is a part.
  - In application of a regulation (e.g., Prevention of money laundering and terrorism funding).
  - To protect vital interests of a person or to perform tasks in defense of public interest.

- To avoid conflicts, it's better to **ask for consent**

Penalties

- Minor infractions
  - Up to 40.000€
  - E.g.: asking for payment to exercise ARCO rights, or not attending requests
- Serious infractions
  - Up to 300K €:
  - E.g., processing child data without consent, not adopting measures for data security
- Severe infractions
  - Up to 20M €:
  - E.g.; Not cooperate or ignore AEPD instructions, infringe secrecy, not blocking data when requested, transferring data to third countries without data protection guarantees…

Example

Home » CNIL Fines Google And Amazon 135 Million Euros For Alleged Cookie Violations

CNIL Fines Google and Amazon 135 Million Euros for Alleged Cookie Violations

Posted on December 14, 2020

POSTED IN ENFORCEMENT, EUROPEAN UNION, INTERNATIONAL

On December 10, 2020, the French Data Protection Authority (the "CNIL") announced that it has levied fines of €60 million on Google LLC and €40 million on Google Ireland Limited under the French cookie rules for their alleged failure to (1) obtain the consent of users of the French version of Google's search engine (google.fr) before setting advertising cookies on their devices; (2) provide users with adequate information about the use of cookies; and (3) implement a fully effective opt-out mechanism to enable users to refuse cookies. On the same date, the CNIL announced that it has levied a fine of €35 million on Amazon Europe Core under the

Roadmap

1. Rule hierarchy
2. European rules
    1. GDPR
3. Spanish rules
    1. **Constitution**
    2. LOPDGDD

Constitution

- *Art. 18*
  - *The law shall **limit the use of data processing** in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights.*
  - *https://www.boe.es/legislacion/documentos/ConstitucionINGLES.pdf*
- Constitutional Court Sentence 94/1998:
  - **Right to Data Protection:** Citizens can oppose to certain personal data being used for different purposes to those that justified their collection.
- Constitutional Court Sentence 292/2000:
  - Right to Data Protection as a ***Fundamental right, autonomous and independent***: citizens can decide which data they provide to a third party, either the Government or a company, or which data can the third party collect, but also know who has access to those data and oppose to that access or usage.

Roadmap

1. Rule hierarchy
2. European rules
    1. GDPR
3. Spanish rules
    1. Constitution
    2. **LOPDGDD**

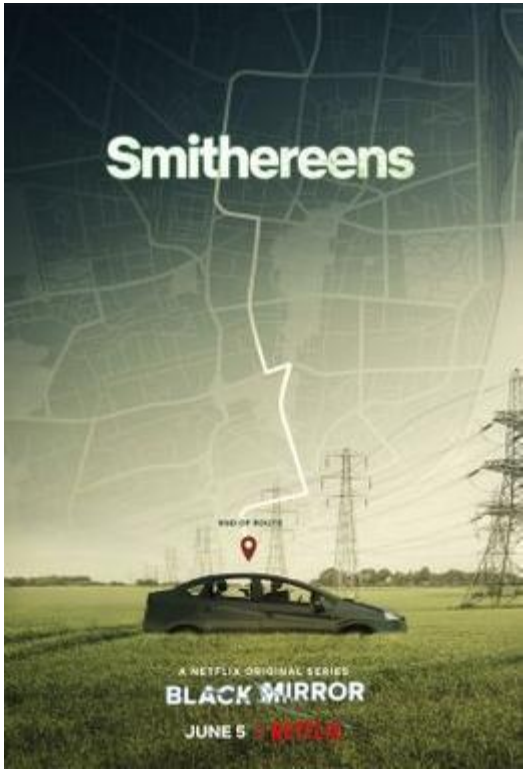
New LOPD

- Repeals the former Organic Law 15/1999, of December 5th, on data protection (LOPD)
- Organic Law 3/2018, of December 5thon Data Protection and Guarantee of Digital Rights.
- Its purpose is to adapt the Spanish law to the GDPR

https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

Data of deceased people

- Family and heirs might request for access to personal data of deceased people, except if they forbid it explicitly, or if a law prevents it



Business with mandatory DPO

1. Professional colleges.
2. Learning centres, including private and public Universities.
3. Health centres.
4. Companies that exploit networks and offer electronic communications services, when they process personal data sistematically in a large scale.
5. Information system providers who profile users in a large scale.
6. Credit financial establishments.
7. Insurance companies.
8. Companies that provide investment services.
9. Distributors and marketers of electric power and gas.
10. Entities responsible for files related to patrimonial solvency, fraud prevention, money laundering or terrorism funding.
11. Companies that perform publicity and marketing, when they evaluate user profiles and process data according to user preferences.
12. Entities that issue commercial reports on natural people.
13. Gambling and betting operators that provide their services through electronic, telematic, interactive and computerized channels.
14. Private security companies.
15. Sports federations that process child data

druiz@us.es
inmahernandez@us.es

Languages and computer systems department

University of Seville

UNIVERSIDAD D SEVILLA